



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/669,452

09/24/2003

Mark L. Buer

50493/SDB/B600

4590

23363 7590 08/08/2008
CHRISTIE, PARKER & HALE, LLP
PO BOX 7068
PASADENA, CA 91109-7068

EXAMINER

HOMAYOUNMEHR, FARID

ART UNIT

PAPER NUMBER

2139

MAIL DATE

DELIVERY MODE

08/08/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/669,452	Applicant(s) BUER ET AL.	
	Examiner Farid Homayounmehr	Art Unit 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 11 April 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-9 and 12-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-9, 12-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is responsive to communications: application, filed 9/24/2003; amendment filed 4/11/2008.
2. Claims 1-9, 12-19 are pending in the case.

Response to Arguments

3. Applicants' arguments with respect to claim rejections have been fully considered, but they are not persuasive.

Applicant argues that Ziai's item 411 (419) and 403 do not share an input buffer, and concludes that the new feature of an input buffer shared among input ports is not taught by the combination of Ziai and Anand. However, as show in the new grounds of rejection, buffers 403 and 419 share a network interface. Network interfaces include a buffer to output data to connect the output data to the interfacing unit.

Applicant further argues that Ziai does not teach "a security association lookup unit configured to identify a security association address in a first portion of an address space associated with the cryptography accelerator by using header information, the first portion of the address space corresponding to bus controller memory, wherein the

security association lookup unit is operable to acquire the security association information from bus controller memory,". Applicant cites different portions of Ziai to conclude that SPD and SAD located in the onchip memory. Applicant then references their Specification to point out that obtaining security association information from the bus controller memory has certain advantages. However, none of these statements traverse the rejection associated with the said limitation. Note that as defined in applicant's Specification page 21, lines 9-11, a bus controller memory is any memory associated with a mechanism interconnecting devices in a computer system. As indicated in the rejection, the security association information in Ziai is received from a memory controlled by the DMA, which interconnects different devices in a computer system.

Based on the discussion above, applicant's argument relative to allowability of claims is found non persuasive.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1-9, 12-19 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to

one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The amended claims include “each cryptographic processing core having a plurality of data paths”. The Specification does not specifically define a data path, and the example cited for a data paths points to cryptographic processing cores in Fig. 3. It is not clear how a data path is distinguished from a cryptographic processing core. The Specification does not describe a cryptographic processing core having plurality of data paths.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-9 and 12-19 rejected under 35 U.S.C. 103(a) as being unpatentable over Ziai (US Patent No. 7,017,042, filed June 14, 2001), and further in view of Anand (U.S. Patent No. 7,266,703, filed Dec. 10, 2001)

7.1. As per claim 1, Ziai is directed to a cryptography accelerator (abstract, or items 402 or 411 in Fig. 4), comprising: a plurality of input ports configured to receive a data sequence comprising header information and payload information from an entity external to the cryptography accelerator (Fig. 4, items 401 or 412 and associated text

Art Unit: 2139

describe a network interface which receives/sends data packets from/to the network); a plurality of cryptographic processing cores, (Ziai teaches a cryptographic processing core, but does not explicitly indicate a **plurality** of cores. However, it would have been obvious to the one skilled in art to use multiple cryptographic cores to improve the speed of cryptographic processing. This is shown in Anand Fig. 1 and 2 and associated text, where a cryptographic core is shown to handle 4 independent channels. Fig. 2 item 208 also shows a buffer shared by input ports, which sends the packets from different channels for cryptographic processing (hashing) to the core. Also, col. 21 lines 47-52 clearly shows the option of multiple cores to perform cryptographic process to improve the speed. The combination of Anand's teaching of multiple input ports and cryptographic cores with Ziai would have been obvious to the one skilled in art, because the two references are analogous art, and the motivation to combine would be to improve the speed of cryptographic process.), each cryptographic processing core having a plurality of data paths (see Anand Fig. 7, showing cryptographic cores 702, 704 and 706 having several data paths); an input buffer shared among the plurality of input ports and the plurality of data paths associated with each cryptographic processing core in the plurality of cryptographic processing cores, the shared input buffer configured to hold payload information associated with the data received by the plurality of input ports (Fig. 4, items 403 or 419 and associated text. Note that items 403 and 419 share the output buffer from the network interface, which connects the packets from the network to device 400); and a security association lookup unit configured to identify a security association address in a first portion of an address space associated

with the cryptography accelerator by using header information (col. 6, line 17-43), the first portion of the address space corresponding to bus controller memory wherein the security association lookup unit is operable to acquire the security association information from bus controller memory (the security association information is obtained from the IPSEC security association data base (item 420, Fig. 4), which works with the cryptographic accelerator (item 402 or 411) and is associated with the DMA controller. DMA controller takes control of the bus and memory for data transfer between devices).

7.2. As per claim 2, Ziai is directed to the cryptography accelerator of claim 1, wherein the security association lookup unit identifies the security association address using header information associated with the received data sequence (col. 6, line 4-10).

7.3. As per claim 3, Ziai is directed to the cryptography accelerator of claim 2, wherein the security association lookup unit identifies the security association address by performing a hash on the header information (see response to claim 2, and note that hashing to create an index to identify the address of data located in memory was a standard and widely used procedure in database systems at the time of invention).

7.4. As per claim 4, Ziai is directed to the cryptography accelerator of claim 2, wherein the security association lookup unit identifies the security association address by performing a hash using a source address, a destination address, a SPI, a source

port number, and a destination port number (see response to claim 2 and col. 6, lines 4-10).

7.5. As per claim 5, Ziai is directed to the cryptography accelerator of claim 4, wherein the hash further uses protocol information and a version number (per col. 6, line 4-10, the information used to determine the security association address is IP addresses. Therefore, the protocol data (IP) and its version (IP version 4 and IP version 6 have different addressing scheme) are part of information).

7.6. As per claim 6, Ziai is directed to the cryptography accelerator of claim 1, wherein the first portion of the address space is a HyperTransport address space (HyperTransport links connect devices in ICs. Item 415 in Fig. 4 is a link between IC devices, and is separate from the system bus (col. 7, line 65-70).

7.7. As per claim 7, Ziai is directed to the cryptography accelerator of claim 1, wherein the first portion of the address space is a Peripheral Components Interface (PCI) address space (Fig. 4 item 405 is a peripheral memory, with a peripheral address space).

7.8. As per claim 8, Ziai is directed to the cryptography accelerator of claim 7, wherein a second portion of the address space corresponds to a system memory address space, the random access memory coupled to a CPU external to the

cryptography accelerator (Fig. 3A item 307 and associated text, which is a memory separate from the accelerator memory space).

7.9. As per claim 9, Ziai is directed to the cryptography accelerator of claim 8, wherein a third portion of the address space corresponds to on-chip memory (col. 4, line 62-66).

7.10. Claims 10 and 11 were cancelled by the applicant.

7.11. Limitations of claims 12-19 are substantially the same as limitations of claims 1-9 above, and noting that Ziai teaches processing the second packet without waiting for the result of the read request for the first packet. This is taught by Ziai in col. Line 1-3, where it is determined if the packet requires IPSec processing. Per col. 6 lines 4-16, packets that do not require IPSec processing may bypass the decryption process performed by the accelerator, and therefore be processed without waiting for result of the packets in front of it that require IPSec processing and decryption. Ziai also teaches plurality of cryptographic processing data paths as required by claim 13. As shown in col. 6 lines 17 to col. 7 line 24, packets go through different paths based on their security policy needs. For example, packets with ESP mode have different processing requirements than those with AH protocol. Note that the purpose of Ziai's invention is to free up system resources from having to wait for the results, or perform the cryptographic process requirements, by deploying additional cryptographic accelerators.

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is (571) 272-3739. The examiner can be normally reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

8/1/2008

/Kristine Kincaid/

Supervisory Patent Examiner, Art Unit 2139

Application/Control Number: 10/669,452
Art Unit: 2139

Page 11